Extended Abstract: Cross-Layer Jamming Detection and Mitigation in Wireless Broadcast Networks

Jerry T. Chiang Yih-Chun Hu
Department of Electrical and Computer Engineering
University of Illinois, Urbana-Champaign
1406 W. Green St., Urbana, IL 61801-2918
{chiang2, yihchun} @uiuc.edu

ABSTRACT

Mobile communication systems are often susceptible to high level of noise injected by adversaries, known as jamming attack. Jamming is difficult to prevent in broadcast networks because a user that can decode a transmission can also jam the transmission. In this paper, we describe a *code tree* system that helps the physical layer circumvent jammers. This system works with any spread-spectrum communications system. In our system, the transmitter has more information than any single receiver. Each receiver cooperates with the transmitter to detect any jamming that affects that receiver. Our scheme mitigates the jamming attack while allowing the transmitter to transmit on fewer codes than the number of users. We simulated our system in a theoretical setting using MATLAB. The result shows significant improvement over naively transmitting on a single shared code.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*Security and protections, (e.g., firewalls)*; C.2.2 [**Computer-Communication Networks**]: Network Protocols—*Protocol architecture (OSI model)*

General Terms

Security, Performance

1. INTRODUCTION

Mobile communication systems are often susceptible to the jamming attack in which adversaries attempt to overpower transmitted signals by injecting a high level of noise, lowering the signal-to-noise ratio (SNR), thereby reducing the probability of successful packet reception. Previously proposed approaches to jamming reside entirely at the physical layer. However, substantial previous work shows that upper-layer feedback can improve lower-layer performance in areas such as transmit power control [4]. We present the first cross-layer solution that uses an upper-layer security protocol and physical layer processing gain to achieve substantial improvement over existing solutions.

One effective countermeasure to the jamming attack is *spread spectrum* [13], in which a transmitter redundantly encodes information using a *code*, allowing a receiver to reject signals that do not come from the transmitter. One example of spread spectrum is *Fast Frequency Hopping Code Division Multiple Access* (FFH-CDMA) where the entire spectrum is divided into a number of frequency bands and each user is assigned a *frequency hopping pattern*. The user remains on any frequency band for one time slot, the duration of which is much shorter than the time it takes to send one bit, and changes frequencies according to its frequency hopping pattern.

At each time slot, a jammer must choose one or more frequency bands to jam. If it chooses too many bands, then its effective power in each band is substantially reduced. On the other hand, if the jammer fails to jam on most of the frequency bands specified in the hopping pattern, then the legitimate signal will have much higher received power level than the jamming signal, and is very likely to be successfully received. The frequency hopping pattern can thus be viewed as a *secret key* between the sender and the receiver, such that a jammer without the key is unable to effectively jam a message sent on that pattern. A further benefit of transmitting in smaller frequency bands is that users will also receive less interference from noise.

Furthermore, FFH-CDMA allows its users to use multiple frequency hopping patterns simultaneously. For example, to simultaneously transmit the same packet on two frequency hopping patterns, a sender divides its power across the two frequency bands specified in the patterns. If the two patterns have a time slot in which they share a band, then the sender can use its full power on a single band during that time slot. To simultaneously receive on two frequency hopping patterns, a receiver simply monitors the two frequency bands.

The ability of spread spectrum systems to simultaneously transmit and receive have long been used in commercial systems such as IS-95 [7]. Though IS-95 is not suitable for use in an adversarial environment due to the use of fixed and published codes, recent work by Li et al [8] uses AES to generate unpredictable, time-varying codes from fixed, secret codes. We assume the use of equivalent time-varying hopping patterns to eliminate the security flaws inherent in using fixed patterns over an extended period of time.

Though FFH-CDMA can be highly effective against jamming in point-to-point communication systems in which a single sender transmits to a single receiver, it is difficult to prevent jamming in a broadcast system that transmits information to multiple users at once. This is because if the jammer discovers the hopping pattern in use (for exam-

MobiCom'07, September 9–14, 2007, Montréal, Québec, Canada.
ACM 978-1-59593-681-3/07/0009.

ple, by compromising a receiver), all benefit of using CDMA against jamming is lost. There are two basic ways to achieve point-to-multipoint communications: first, a sender can use a single code to transmit to all receivers; alternatively, a sender can use one hopping pattern for each receiver. When a single hopping pattern is used, every legitimate receiver must have that hopping pattern, including any adversarial receivers, making it substantially easier for the jammer to acquire the hopping pattern and overcome the benefits of CDMA. Conversely, when an individual hopping pattern is used for each receiver, transmission is less power efficient since the total transmitted power is divided between hopping patterns. Hybrid schemes are also possible, where each hopping pattern is shared by several receivers, reducing the number of hopping patterns in the system. The usage of number of hopping patterns is highly related to the symmetry of the system and will be discussed more in depth in Section 3.1.

In this paper, we describe a binary tree structure implemented above the physical layer that takes advantage of the unique properties of code sequences in order to provide an anti-jam broadcast system based on any existing code sequence spread spectrum communication systems. We will show that this structure can achieve nearly as much packet delivery success as when the jammers know no code sequences.

For purposes of simplicity, we describe our protocol within the context of a Fast-Frequency-Hopping CDMA system; however, our solution can be generalized to other CDMA systems including Direct-Sequence CDMA and Orthogonal Frequency Division Multiplexing (OFDM). In fact, our work has broad applicability to a wide variety of existing wireless access technologies such as IEEE 802.11 [3], IS-95 [7], and cdma2000 [5], that are already CDMA systems.

Section 2 overviews the related work. In Section 3, we describe how we mitigate jamming, and we improve this approach in Section 4. Section 5 presents the results of an evaluation of our approach using MATLAB, and Section 6 concludes.

2. RELATED WORK

Jamming prevention using CDMA has been studied at length [13]. Other physical layer techniques, such as the use of multiple antennas, have also been studied, but those do not make use of higher-layer feedback and are orthogonal to our approach.

Asymmetric cryptography [9], such as RSA [11] and Diffie-Hellman [2], rely on the alleged asymmetry of certain computational functions to achieve public-key cryptography and digital signatures. Our work differs in that it overlays an inherently symmetric operation: wireless transmission. Other work has used time and delayed disclosure to provide asymmetry [10, 6]. If we do this with spreading codes (as described by Kuhn [6]), we still need a jam-resistant way to provide receivers with a spreading code.

The effectiveness of jamming [1] and the difficulty of differentiating jamming from congestion [14] have previously been discussed, but they do not propose solutions to traverse the jammed area. In particular, Xu et al [14] try to detect and avoid jammed regions.

To algorithmically detect and avert jamming, we take advantage of the tree structure proposed by several key management methods. In particular, Sherman and McGrew [12]

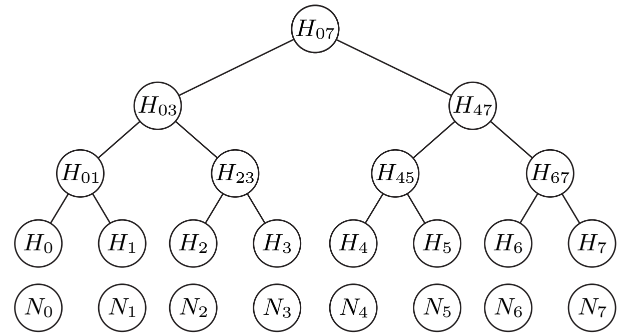

Figure 1: Example Code Tree

proposed a binary key tree where each leaf corresponds to a single user, and each user possesses the keys corresponding to all ancestors of that leaf. Our work uses a similar structure (Section 3) but contributes novel techniques of particular value in wireless networks, including jamming detection and tree recombination.

3. TREE CODING SCHEME

3.1 Symmetry of Hopping Patterns

The current use of hopping patterns in a FFH-CDMA system is analogous to a *symmetric-key cryptosystem*, in which an encryption code and decryption code are easily derivable from each other. For example, in the FFH-CDMA system, encoding and decoding both use the same hopping pattern. By keeping each hopping pattern a secret between the transmitter and receiver, the hopping pattern effectively serves as a cryptographic key for both encryption and decryption. This symmetry presents significant challenges to the design of a broadcast system: a symmetric key should not be shared, otherwise a single compromised user can jam in a way that cannot be rejected by frequency hopping.

3.2 Tree-Based Approach

In this section, we describe our approach to create an asymmetric system that allows detection and isolation of jammers in a spread-spectrum system. This approach is similar to the key tree proposed by Sherman and McGrew [12]. Each transmitter builds a balanced binary tree of randomly generated hopping patterns. The transmitter associates each legitimate receiver with a unique leaf in this binary tree, and gives this receiver the hopping patterns corresponding to that leaf and all ancestors of that leaf in the tree. For example, in Figure 1, user N_2 would have access to hopping patterns H_2, H_{23}, H_{03}, and H_{07}.

When there are no jammers, a transmitter can transmit on a single hopping pattern; specifically, it would choose the hopping pattern corresponding to the root of the tree. Transmissions on this hopping pattern can be decoded by any legitimate receiver. For example, in Figure 1, the transmitter would send on hopping pattern H_{07}. In general, in order to ensure that every receiver can decode the packet while ensuring power efficiency, the transmitter wants to transmit on a set of hopping patterns such that any user can decode using exactly one hopping pattern in the set. We call such set a *disjoint cover*. Once jamming has been detected on some hopping patterns (we discuss jamming detection in Section 3.3), the transmitter should avoid using such hopping patterns in the future. Because each extraneous hopping pattern used for transmission either increases the total power consumption or reduces the average received signal strength on each hopping pattern, we want to transmit on the smallest possible set of hopping patterns on which no jamming was detected.

3.3 Jamming Detection Algorithm

When the transmitter sends a packet, it will do so on the minimal disjoint cover on which no jamming had been previously detected, so that all legitimate receivers can decode the packet. In order to detect additional jammers, the transmitter additionally transmits on a *test* hopping pattern, which it randomly chooses from among the descendants of the cover. This redundant test hopping pattern allows the transmitter and receiver to cooperatively detect jamming on any hopping pattern in the cover that is an ancestor of the test hopping pattern. We call this ancestor the *detectable* hopping pattern.

If no jammers are present, each user should get either one or two identical messages, the first encoded using one of the patterns from the cover, and possibly a second encoded using the test hopping pattern. If any user receives the second message without receiving the first message, then it should suspect jamming on the detectable hopping pattern. Any user detecting jamming in this way should report that finding to the transmitter, for example by transmitting a JAMMING DETECTED message using the leaf hopping pattern shared between the transmitter and the detecting receiver (because no jammer knows that leaf hopping pattern). In some instances, jamming on the detectable hopping pattern will not be detected. This can happen either when a jammer jams on the test hopping pattern or when no normal users know the test hopping pattern.

Testing can be generalized so that a *set* of test hopping patterns are used at each step, thus allowing a *set* of detectable hopping patterns. For example, if the current disjoint cover in use is $\{H_{03}, H_{45}, H_{67}\}$, then the test code set of $\{H_{01}, H_4\}$ would make the detectable set be $\{H_{03}, H_{45}\}$.

Response to Jamming.

When a transmitter detects jamming, it will choose a different cover. In particular, if jamming is detected on some hopping pattern h in the current cover, the transmitter will remove h from the cover and add the two children of h to the cover. For security reasons, jamming reports are only accepted from hosts that should know hopping pattern h. For example, in Figure 1, when jamming is detected on pattern H_{07}, the transmitter splits the cover into $\{H_{03}, H_{47}\}$. If jamming is further detected on H_{47}, the resulting cover would be $\{H_{03}, H_{45}, H_{67}\}$.

4. PARAMETER CHOICE

The safest technique for choosing test hopping patterns is to pick leaves because jammers do not have access to their siblings' patterns. However, when only a small fraction of a transmitter's legitimate receivers are within range, many tests are wasted because the test hopping patterns belong to absent users who cannot report jamming. If we choose test hopping patterns that are too close to the root, there is a greater probability that jammers will have the test hopping pattern. In this section we analyze the tradeoffs between these two extremes.

Each legitimate receiver can be characterized as either *absent*, *normal*, or a *jammer*. The root of a subtree is jammed if any of the leaves of that subtree are jammers; the root of a subtree is absent if all of the leaves of that subtree are absent; and otherwise the root of the subtree is considered normal. These designations reflect how the network will react when the root of that subtree is chosen as a test hopping pattern.

We consider the following algorithm for testing: we first test hopping patterns at a height of M, and if jamming is not detected on any of those patterns, we then test at height $M-1$. If we assume that the set of tests at each height is independent and identically distributed, we can derive, at height M, the probability of detection $P_M[d]$ and the expected steps until detection $E_M[d]$, given there are 2^n total users, of which A are absent, $J > 0$ are jammers, and $N > 0$ are normal.

$P_M[d]$ can be calculated because detection happens at the root of a normal subtree. Because a height M subtree has 2^M users, there are $\binom{2^n}{2^M}$ choices of users for that subtree. Of these choices, there are $\binom{2^n-J}{2^M}$ choices to have no jammer in this subtree. We must subtract from this the number of ways of making an absent subtree, which is $\binom{A}{2^M}$. Therefore

$$P_M[d] = \frac{\binom{2^n-J}{2^M} - \binom{A}{2^M}}{\binom{2^n}{2^M}}$$

$E_0[d]$ can also be calculated combinatorially. The calculation is similar to that of a geometric distribution. At height 0, all nodes are leaf nodes, and when testing leaf nodes, the probability of detecting jamming on the first test is the same as the probability of selecting a normal user. The probability of detecting jamming on the second test is equal to the probability of selecting an absent user or a jammer on the first test and then selecting a normal user on the second test. Extending this idea, the expected detection time is a weighted sum of detection probabilities. We sum only over $2^n - 2$ terms since there are only 2^n users and at least one of them is a jammer and another one a normal user. Then $E_0[d]$ is given by

$$\frac{N}{2^n} + \sum_{j=0}^{2^n-3} (j+2) \left(\prod_{i=0}^{j} \frac{2^n - N - i}{2^n - i} \right) \left(\frac{N}{2^n - j - 1} \right)$$

$E_M[d]$ is then calculated recursively since the testing rule moves the testing level down when testing at level M is unsuccessful. The first half of the equation resembles $E_0[d]$, except that it is performed at height M. The second term is a penalty for non-detection at height M: this penalty consists of a part for wasting 2^M steps at height M and a recursive term for the expected number of detections at height $M-1$.

$$\begin{aligned} E_M[d] \;&=\; P_M[d] \sum_{i=0}^{2^{n-M}-1} (i+1)(1-P_M[d])^i \\ &\quad + (1-P_M[d])^{2^{n-M}} \left[2^M + E_{M-1}[d] \right] \end{aligned}$$

The goal of the transmitter is to choose M that minimizes $E_M[d]$.

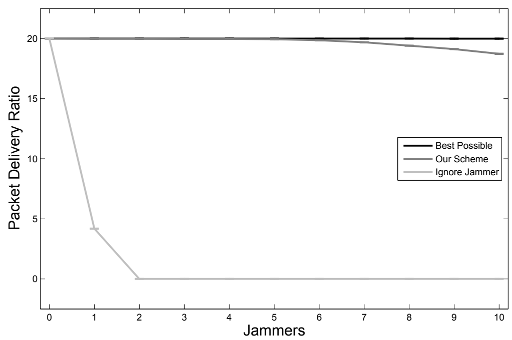

Figure 2: Packet Delivery Ratio

5. EVALUATION

We performed a MATLAB simulation on the theoretical performance of our tree coding scheme. The simulation scenario consists of one base station, 20 normal users, and 0 to 10 jammers. The total jamming power at each receiver is equal to the number of jammers times the total received base station power (that is, each jammer is as powerful as the base station). Jammers that emit more power can be modeled by increasing the number of jammers. To make decoding more challenging, we assumed an additive white Gaussian noise whose power is 15dB higher than the total power from the base station at each receiver *over the entire frequency occupied by the FFH-CDMA system.* This is not an unrealistic scenario as spread spectrum systems often operate under noise floor. We implemented the spread spectrum system using FFH-CDMA with 127 channels and 63 hops per bit. Each jammer in this system allocate all power to jamming the frequency band specified in the frequency hopping pattern of the cover. For each number of jammers, we performed 10 tests of 10,000 6-bit messages transmitted by the base station.

We simulated three jamming mitigation strategies. The first strategy, which we call "Ignore Jamming," transmits to all receivers on a single hopping pattern. The second strategy, which we call "Our Scheme," reflects the scheme described in Section 3. Our final strategy, which we call "Best Possible," contemplates a protocol in which the jammer never has access to the root hopping pattern (for example, if the transmitter has a hopping pattern for each set of users, and omnisciently knows which codes the jammer has, even before the jammer uses them). In this strategy, we send on a single hopping pattern, and each jammer jams on a random hopping pattern.

Figure 2 shows the results of our simulation. We computed the packet delivery ratio (PDR) by dividing the number of packets received by the number of packets sent. For each jamming strategy and number of jammers, we plot the average and 95% confidence interval on the packet delivery ratio. Because we had 20 normal users in each scenario (in addition to the transmitter and jammers), and because all normal users are within wireless transmission range of the transmitter, the best possible result is a packet delivery ratio of 20. This graph shows that when jammers have no knowledge of the hopping pattern in use, the system is able to deliver almost 100% of packets by using only one hopping pattern. However, if the system only uses one hopping pattern and such knowledge is compromised by any jammer, the system degrades rapidly. Our scheme also delivers almost 100% of packets when there are five jammers or fewer and delivers more than 90% of packets between six to ten jammers even when jammers gain knowledge of codes used by the system.

6. CONCLUSIONS

This paper described a tree-based coding mechanism that can detect jamming and reconfigure to reduce the impact of jammers. We showed that the parameter choice of testing level may affect the efficiency of the system, and subsequently optimized this parameter. We also presented results simulated in a theoretical setting that showed the performance advantage of tree coding, and that jamming can be efficiently and effectively detected and circumvented in a wireless broadcast network.

7. REFERENCES

[1] Timothy X Brown, Jesse James, and Amita Sethi. Jamming and sensing of encrypted wireless ad hoc networks. Technical Report CU-CS-1005-06, University of Colorado at Boulder, 2006.

[2] Whitfield Diffie and Martin E. Hellman. Privacy and authentication: An introduction to cryptography. *Proceedings of the IEEE*, 67(3):397–427, March 1979.

[3] IEEE Computer Society LAN MAN Standards Committee. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11-1997.* The Institute of Electrical and Electronics Engineers, New York, New York, 1997.

[4] V. Kawadia and P. Kumar. Power control and clustering in ad hoc networks. In *Proceedings of the Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003)*, March 2003.

[5] D. N. Knisely, S. Kumar, S. Laha, and S. Nanda. Evolution of wireless data services: IS-95 to CDMA2000. *IEEE Communications Magazine*, 36(10):140–149, October 1998.

[6] Markus G. Kuhn. An asymmetric security mechanism for navigation signals. In *Proceedings of the 6th Information Hiding Workshop*, volume 3200, pages 239–252, May 2004.

[7] J. S. Lee. Overview of the technical basis of Qualcomm's CDMA cellular telephone system design: a view of North American TIA/EIA IS-95. In *Proc ICCS '94*, volume 2, pages 353–358, November 1994.

[8] Tontong Li, Jian Ren, Qi Ling, and Anil Jain. Physical layer built-in security analysis and enhancement of CDMA systems. In *Proceedings of the Military Communications Conference, 2005. MILCOM 2005. IEEE*, pages 956–962, October 2005.

[9] R. Merkle. Secure communication over insecure channels. *Communications of the ACM*, 21(4):294–299, 1978.

[10] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, and J. D. Tygar. SPINS: Security protocols for sensor networks. In *Seventh Annual ACM International Conference on Mobile Computing and Networks (MobiCom 2001)*, Rome, Italy, July 2001.

[11] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[12] Alan T. Sherman and David A. McGrew. Key establishment in large dynamic groups using one-way function trees. *IEEE Transactions on Software Engineering*, 29(5):444–458, May 2003.

[13] A. J. Viterbi. *CDMA Principles of Spread Spectrum Communication.* Addison-Wesley, 1995.

[14] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In *Proceedings of The 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2005)*, pages 46–57, May 2005.